<center>REMARKS</center>

Claims 1–20 are pending in the application, with claims 1, 15, and 18 being the independent claims.

Claims 1 and 15–20 stand rejected under 35 USC §103 as unpatentable over the article "IBM Cryptolopes, Super Distribution and Digital Rights Management" (Kaplan) in view of the United States Patent No. 6,021,491 (Renaud). Claims 2–14, 16, 17, 19, and 20 also stand rejected under 35 USC §103 as unpatentable over Kaplan in view of Renaud and further in view of U.S. Patent No. 5,894,320 (Vancelette). Applicant traverses these rejections.

According to one aspect of Applicant's invention, independent claim 1 recites a method for managing a scrambled event of a service provider. The method features receiving in a device an electronic list of events, at least one event having a digitally signed encrypted message associated therewith. The encrypted message includes a descrambling key and event information. The method also features receiving in the device, in response to user selection of the event, the digitally signed encrypted message. The method also includes authenticating in the device a source of the digitally signed encrypted message in response to receipt of the digitally signed encrypted message, and decrypting in the device the digitally signed encrypted message to obtain the descrambling key upon the authentication. The method also features receiving in the device the selected event from the service provider, the selected event being scrambled using the descrambling key for preventing unauthorized access to the selected event, and descrambling in the device the selected event using the descrambling key.

In another aspect of Applicant's invention, independent claim 15 recites a method for managing access between a device having a smart card coupled thereto and a service provider. The method includes a step of receiving an electronic program from a guide provider, the guide having a message and a digital signature associated with each event in the guide, the message being encrypted using a public key of the smart card and the digital signature being created using a private key of the guide provider. The method also includes selecting an event from the guide; receiving the encrypted message and the digital signature corresponding to the selected event; authenticating the guide provider by decrypting the digital signature using a public key of the guide provider, the guide public key being stored in the device; passing the message to the smart card; decrypting, in the smart card, the message using a private key of the smart card to obtain event information and a symmetric key, the smart card private key being stored within the smart card; storing the event information in the smart card and updating account information based on the event information; receiving from the service provider the selected event, the selected event being scrambled using the symmetric key; and descrambling in the smart card, the selected event using the symmetric key to generate a descrambled event.

In a still further aspect of the invention, independent claim 18 recites a method for managing access between a device having a smart card coupled thereto and a service provider. The method includes receiving an electronic program guide from a guide provider, the guide having a digital certificate and a separate message corresponding to each event in the guide. Each of the digital certificates is encrypted using a first private key of the guide and the separate

3

message being encrypted using a public key of the smart card and having an associated digital signature created using a second private key of the guide. The method also includes selecting an event from the guide; receiving the digital certificate, the message and the digital signature corresponding to the selected event; and authenticating the guide provider by decrypting the digital certificate using a first public key of the guide to obtain a second public key of the guide, and decrypting the digital signature using the second guide public key, the first guide public being stored in the device. Furthermore, the device features passing the message to the smart card; decrypting in the smart card the message using a private key of the smart card to obtain event information in a symmetric key, the smart card private key being stored within the smart card; storing the event information in the smart card and updating account information based on the event information; receiving from the service provider the selected event, the selected event being scrambled using the symmetric key; and descrambling in the smart card the selected event using the symmetric key to generate the descrambled event.

Accordingly, independent claim 1 recites a method featuring the steps of authenticating in the device a source of a digitally signed encrypted message in response to receiving a digitally signed encrypted message, and decrypting in the device the digitally signed encrypted message to obtain a descrambling key upon authentication. The method according to independent claim 15 recites authenticating a guide provider by decrypting a digital signature using a public key of the guide provider, the public key being stored in the device; passing the message to the smart card; and decrypting in the smart card the message using a private key of the smart card to obtain event information and a symmetric key,

4

the smart card private key being stored within the smart card, and the symmetric key being used to descrambled the selected event to generate a descrambled event. The method of claim 18 features authenticating a guide provider by decrypting a digital certificate using a first public key of the guide to obtain a second public key of the guide, and decrypting the digital signature using the second guide public key, the first guide public key being stored in the device.

Applicant submits that at least these features are not taught or suggested by the cited documents, whether those documents are taken alone or in combination. Specifically, nowhere are the cited documents understood to teach or suggest the authenticating of a source as recited in independent claim 1 or the authenticating of a guide provider as recited in claims 15 and 18.

The Kaplan reference is understood to teach a cryptographic envelope used to disseminate information that is not to be given away for free. As described in more detail beginning on page 3 of the reference, the cryptographic envelope is a digital package including an abstract, encrypted parts, key records corresponding to the encrypted parts, encrypted fingerprinting and watermarking instructions, terms and conditions, and authenticity with digital signatures. As set forth on page 5 in the discussion of the section, Authentication with Digital Signatures, "each Cryptolope contains information so that its (potential) users can authenticate its entire contents. In addition, the "user or clearing center can verify the authenticity of any part of a Cryptolope by first checking the digital signature on the BOM." Moreover, on page 7 of the reference, under the heading, "Buying a Cryptolope," numeral 2 indicates that the royalty clearing center verifies the authenticity of terms and

5

conditions and key records. However, nowhere is Kaplan understood to teach or suggest authenticating a source of a digitally signed encrypted message in response to receiving a digitally signed encrypted message, and decrypting the digitally signed encrypted message to obtain the descrambling key upon the authenticating, as rected in independent claim 1. Kaplan is understood only to teach authenticating contents of a package of information contained in a bill of materials.

Similarly, Kaplan is not understood to teach or suggest authenticating a guide provider by decrypting a digital signature using a public key of the guide provider, with the guide public key being stored in the device and decrypting the message using a private key of the smart card to obtain event information and the symmetric key, the smart card private key being stored within the smart card, as recited in independent claim 15. And, Kaplan is not understood to teach or suggest authenticating a guide provider by decrypting a digital certificate using a first public key of the guide to obtain a second public key of the guide, and decrypting the digital signature using the second guide public key, as recited in independent claim 18. As noted above, Kaplan is understood only to teach authenticating contents of a digital package on a bill of materials.

Renaud also is not understood to teach or suggest the authenticating features not taught by Kaplan. Renaud is understood to be cited by the Office Action for "disclosing a method, apparatus, and products provided for verifying the authenticity of data within one or more data files. Renaud discloses the user receiving a signed file that it verifies the authenticity of the signed signature file." Page 3, July 14, 2006 Office Action. Without conceding the propriety of the Office Action's characterization of Renaud, that patent is not understood to

teach or suggest authenticating a source of digitally signed encrypted message in response to receiving a digitally signed encrypted message and decrypting the digitally signed encrypted message to obtain the descrambling key upon authentication, as recited in claim 1; or authenticating a guide provider by decrypting a digital signature using a public key of the guide provider, as recited in independent claim 15; or authenticating a guide provider by decrypting a digital certificate using a first public key of the guide to obtain a second public key of the guide, in decrypting the digital signature using the second guide public key, as recited in independent claim 18.

For the foregoing reasons, Applicant submits that the proposed combination of Kaplan and Renaud fails to teach or suggest features of independent claims 1, 15, and 18. Favorable reconsideration and withdrawal of the §103 rejection of these independent claims is therefore requested.

Applicant also submits that neither Kaplan nor Renaud teaches or suggests a smart card. Both claims 15 and 18 are directed to methods for managing access between a device having a smart card coupled thereto and a service provider. Both of those claims also specifically set forth steps including the smart cart. Therefore, the rejections to claims 15 and 18 also cannot stand because neither of the cited documents even mentions a smart card.

Vancelette is understood to be cited merely for teaching features of dependent claims. Without conceding the propriety of the Office Action's characterization of that patent, Vancelette is not understood to remedy the deficiencies of Kaplan and Renaud, discussed above with respect to independent claims 1, 15, and 18.
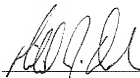
The remaining claims depend from one of the allowable independent claims. These dependent claims are deemed to be allowable by virtue of this dependency, and for reciting other patentable features of applicant's invention. Favorable and independent consideration of the dependent claims are requested.

Applicant submits that this application is condition for allowance. Favorable reconsideration and an early Notice of Allowance are requested.

If necessary, Applicant's below-signed representative may be reached by telephone at (585) 232-6500. All written correspondence should continue to be addressed to the address on file with this application.

Respectfully submitted,

Dated: October 16, 2006
          (Monday)

Michael J. Didas, Registration No. 55,112
Harter Secrest & Emery LLP
1600 Bausch & Lomb Place
Rochester, New York 14604
Telephone: 585-232-6500
Fax: 585-232-2152